Davies du Toit & Associates T/A EyeQ Optometrists

Company Compliance Manual for the Implementation of the Protection of Personal Information Act of 2013

Manual brief & purpose

Our **Company Compliance Manual** refers to our commitment to treat information of customers, employees, stakeholders and other interested parties hereafter referred to as data subjects, with the utmost care and confidentiality in order to protect that information. This is commitment also recognizes the need to balance our obligation against the needs of our society to have access to and process personal information for legitimate purposes, including the purpose of doing business and to provide health care services according to the requirements set by the Health Professionals Act of 1974.

With this policy, we ensure that we process and handle personal information fairly, transparently and with respect towards individual rights.

Where reference is made to the “processing” of personal information, this will include any activity in which the information is worked with, from the time that the information is collected, up to the time that the information is destroyed, regardless of whether the information is worked with manually, or by automated systems.

Scope

This manual refers to all data subjects who provide any amount of information to us.

Who is covered under the Protection of Personal information Act?

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our manual refers to anyone we collaborate with or acts on our behalf and may need occasional access to Personal information that we process.

Compliance Manual elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of the data subjects concerned. All data subjects will be informed of the purpose for which their personal information is being collected. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date.
- Collected fairly and for lawful purpose only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties.
- Processed for the purpose for which it is intended, to enable us to do our work.
- Collected wherever necessary and reasonably through obtained consent
- Collected directly from the person whose information we require, unless;

    (i) The information is of public record

    (ii) The data subject has consented to the collection of their personal information from another source, that does not prejudice the client unfairly

    (iii) The information to be collected in necessary for the maintenance of law and order or national security

    (iv) The information is being collected to comply with a legal obligation including an obligation to SARS

    (v) The information is required to maintain our legitimate business interests

    (vi) Where requesting consent would prejudice the the purpose of the collection of the information

    (vii) Where requesting consent is not reasonably practical in the circumstance

- No longer be processed if required consent is withdrawn, or if a legitimate objection is raised.
- Retained to allow for ;

    (i) **Our obligations under Health Professionals Act of 1974**.
    Medical records to be retained for a period not less than
        - Adults over 21: 7 years
        - Minors: 21 years or up to their 21st birthday, after which 7 years applies.

.

(ii) Our obligations under labour relations act 66 of 1995

- Hiring records **1 year**
- Unsuccessful candidates – **destroyed immediately** after the information is no longer required
- Employees – For **five years** from date of event or after termination of employment
- Employer must keep prescribed details of any strike, lock-out or protest action involving its employees – **Indefinitely -** Section 205(3) Schedule 8, Section 5
- Employers should keep records for each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions - **Indefinitely** -Section 205(3) Schedule 3, Section 8(a)

(iii) Our obligations under the Companies Act 2008

- Five years: counting from the date of submission of a return until the last day of the period. A person required to submit a return but has not complied -indefinitely until the return is complete then for five years

(iv) Continued business operations with interested parties

- Up to five years after our last transaction/interaction

- Destroyed or deleted so as to be de-identified as soon as reasonable possible after request from a data subject in good financial standing and where no conflict arises under the responsibilities imparted on us above.

Our data will not be:

- Further processed where;
  (i) The accuracy of the information is contested, for a period sufficient for us to verify such accuracy
  (ii) The purpose for which it was collected has been achieved and where the personal information is being retained only for the purposes of proof
  (iii) Where the client requests such
  (iv) Where none of the above listed points apply

- Communicated informally
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data

- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

Data Subjects Rights

Our Company recognizes and upholds our data subjects rights to

- Withdraw consent in cases where consent is required
- Object to our processing of information where we are processing it to protect a legitimate interest or to comply with law
- Lodge a complaint regarding our application of POPI with the regulator

Actions

To exercise data protection and to secure the integrity and confidentiality of personal information we're committed to protect it against loss or damage or unauthorized access, through application of the following safeguards:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in POPI, online privacy and security measures
- Build secure networks to protect online data from cyberattacks
  (i) Password secure terminal
  (ii) Email security safeguards to meet GDPR regulations internationally
  (iii) Have firewalls installed at each premises where data is processed
  (iv) Maintain and run antivirus protection
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

- Enter into operator agreements with any third party that might process data on our behalf.

- Our data protection provisions will appear on our website.

Security Breaches

Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, we must notify the Information Regulator and the relevant client/s, unless we are no longer able to identify the client/s. This notification must take place as soon as reasonably possible or within 72 hours of such breach being detected.

Such notification must ;

- Be given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the client/s be delayed.
- Be communicated to the client in writing in one of the following ways, with a view to ensuring that the notification reaches the client:

  (i) by mail to the client's last known physical or postal address;

  (ii) by email to the client's last known email address;

  (iii) by publication on our website or in the news media; or

  (iv) as directed by the Information Regulator.

- Give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and must include:

  (i) a description of the possible consequences of the breach;

  (ii) details of the measures that we intend to take or have taken to address the breach;

  (iii) the recommendation of what the client could do to mitigate the adverse effects of the breach; and

  (v) if known, the identity of the person who may have accessed, or acquired the personal information.

Record Requests

On production of proof of identity, any person is entitled to request that we confirm, free of charge, whether or not we hold any personal information about that person in our records.

If we hold such personal information, on request, we shall provide the person with the record, or a description of the personal information.

Upon payment of a fee of R500-00 plus VAT, including information about the identity of all third parties or categories of third parties who have or have had access to the information. We shall

do this within a reasonable period of time, in a reasonable manner and in an understandable form.

In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have discretion as to whether or not to do so, having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.

If a request for personal information is made and part of the requested information may, or must be refused, every other part must still be disclosed.

A data subject requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request shall be made on the prescribed application form

A data subject is entitled to require us to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully

A data subject is also entitled to require us to destroy or delete records of personal information about them that we are no longer authorised to retain.

In the event that a dispute arises regarding the data subject's rights to have information corrected, and in the event that the subject so requires, we must attach to the information, in a way that it will always be read with the information, an indication that the correction of the information has been requested but has not been made.

We must notify the data subject who has made a request for their personal information to be corrected or deleted what action we have taken as a result of such a request.

Processing of Personal Information of Minors and Dependents

We may only process the personal information of minors or dependents if we have the consent of the child's parent or legal guardian.

Role of the Information Officer

Our Information Officer is Francois du Toit who is our Head Partner. Our Information Officer's responsibilities include:

(i) Ensuring compliance with POPI.
(ii) Dealing with requests which we receive in terms of POPI.
(iii) Working with the Information Regulator in relation to investigations.
(v) To designate in writing as many Deputy Information Officers as are necessary to perform these tasks
(vi) Registering himself and his deputies with the regulator
(vii) Ensure compliance of this manual
(viii) Continues to foster a culture of compliance with POPI within our business
(ix) Develops internal measures and systems to ensure compliance

Circumstance requiring Regulators Authorisation

Certain circumstances will require prior authorisation from the information regulator before processing personal information. The regulator must be notified of our intention to process such information prior to any processing taking place. This includes;

- In the event that processing is required for any purpose other than the original intention for which the data was initially collected
- To process information on criminal behaviour or unlawful or objectionable conduct
- To process information for the purpose of credit reporting
- If we are transferring special personal information of a minor to a third party in a foreign country that does not provide adequate protection of that personal information.

The regulator must make a decision within 4 weeks of such request or upon extension for a period not exceeding 13 weeks. If no decision is forthcoming within this period we can assume the decision is in our favour and will commence with such processing.

Direct Marketing

We may carry out any direct marketing using any form of written or electronic communication to any data subject on proviso of;

- Opportunity was granted for the data subject to object to receiving such marketing material at the time at which their data was collected.

- No objection was made at the time at which their data was collected nor subsequent to receiving any marketing communication from us.
- The marketing material being related to the services and products of our business whose services they have engaged with and provided their information in the context of receiving such services.

Cross Border Information flows

We may not transfer a client's personal information to a third party in a foreign country, unless;

- The data subject consents to, or requests it.
- Such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI, and such third party is governed by similar rules of POPI.
- Such transfer of the personal information is required for the performance of the contract between ourselves and the data subject.
- Such transfer of the personal information is for the benefit of the client and it is not reasonably possible to obtain their consent and that if it were possible the client would be likely to give such consent.

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of information protection guidelines will invoke disciplinary and possibly legal action.

POPI provides for serious penalties for the contravention of its terms. For minor offences a guilty party can receive a fine or be imprisoned for up to 12 months. For serious offences the period of imprisonment rises to a maximum of 10 years. Administrative fines for the company can reach a maximum of R10 million.

Schedules Annexures and Forms

In order to comply with POPI and it's provisions the following forms, documents and contracts exist within our business

- **Company Forms**
  (i) PAIA Manual
  (ii) POPI Manual
  (iii) Form 7 - Information officer registration form
  (iv) Form C - request for information
  (v) Form 3 – Objection to processing of personal information
  (vi) Form 4 – request for correction or deletion of information

- **Customer Forms**
  (i) Customer registration forms
  (ii) Customer consent forms

- **Staff Forms**
  (i) Employee Onboarding forms
  (ii) Employee Code of conduct policy
  (iii) Employee confidentiality policy - included in code of conduct policy
  (iv) EyeQ HR Policy
  (v) Privacy notices Employee data processing
  (vi) Staff confidentiality statement

- **Third Party Processors**
  (i) Operator Agreement forms
  (ii) Operator Compliance statements

- **IT Services**
  (i) Record of antivirus software
  (ii) Record of Firewall
  (iii) Email security protocols